9200/3700

# NOTICE OF APPEAL TO THE
# BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: )
)
Michael MOVALLI et al. )
)
Application No.: 08/679,421 )
) Group Art Unit: 2514
Filed: August 23, 1996 )
) Examiner: M. Tremblay
For: METHOD AND APPARATUS FOR )
GENERATING SECURE )
ENDORSED TRANSACTIONS )

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

## REPLY BRIEF

In support of the timely filed Notice of Appeal filed January 19, 2000, and pursuant to 37 C.F.R. § 1.193, Appellants present in triplicate their reply brief. This is an appeal to the Board of Patent Appeals and Interferences from the decision finally rejecting claims 1-23, 25-27, and 29-31. If any fees are required please charge the deficiencies to our Deposit Account No. 06-0916. If a fee is required for an extension of time under 37 C.F.R. § 1.136 and such fee is not accounted for above, Appellants petition for such an extension and request that the fee be charged to the Deposit Account No. 06-0916.

Appellants hereby incorporate by reference in its entirety their Appeal Brief filed July 21, 2000.

## Issues

The issues presented in this reply brief are:

A. Whether claims 1-4 and 25-27 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith.

B. Whether claims 5-23 and 29-31 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith and further in view of Spies.

## Grouping of Claims

The following groups of claims are considered to be separately patentable:

Group I: Claims 1, 3, and 25-27

Group II: Claims 2 and 4

Group III:  Claims 5-7 and 20-22

Group IV:  Claims 8, 9 and 10

Group V:  Claim 11-14 and 29-31

Group VI:  Claim 15-18

Group VII:  Claim 19

Group VIII:  Claim 23

The groups of claims do not stand or fall together.  The reason Appellants consider the groups of claims to be separately patentable is that the groups of claims define different embodiments of the present invention and define these embodiments in varying levels of detail.

## Argument

**A. Claims 1-4 and 25-27 have been improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over <u>Davies</u> in view of <u>Griffith</u>.**

### 1. <u>Group I: Claims 1, 3, and 25-27</u>

Regarding the rejection of claim 1 as being unpatentable over <u>Davies</u> in view of <u>Griffith</u>, Appellants reiterate that <u>Davies</u> is directed to a simple system involving a "smart card" having its own display and key-pad. The Examiner asserts that certain information provided by the smart card of <u>Davies</u> may be used to uniquely identify an individual, however, the term unique human identifier as defined by Appellants in the specification of the present application is not the broad definition adopted by the Examiner. Appellants may be their own lexicographer and have clearly defined "unique human identifier" in the specification in such a manner that the broad interpretation of that term by the Examiner conflicts with the proper scope of that term.

Understanding that the broader definition of "unique human identifier" is not the proper scope of the claim term the Examiner cites <u>Griffith</u> as teaching a "biometric." The Examiner asserts that "[t]he addition of the biometric taught by Griffith to the check of Davies is as natural a combination as a handwritten signature to a paper check." The Examiner's assertion that a person having ordinary skill in the art would have been motivated to use the finger, voice, retinal pattern, signature, or chemical structure of <u>Griffith</u> in combination with the smart card of <u>Davies</u> is entirely based on a post hoc construction to meet the claimed limitation. There is simply no support in either <u>Griffith</u> or <u>Davies</u> to suggest that the smart card of <u>Davies</u> could or would be used in the manner suggested by the Examiner.

3

As discussed previously, an advantage noted by <u>Davies</u> is that "[t]he PIN is checked by the card and does not enter from a 'foreign' keypad." To add the necessary equipment to capture the finer, voice . . . information of <u>Griffith</u> to the smart card of <u>Davies</u> is simply not reasonable. The information would necessarily have to come from an external source, which would defeat a specific advantage noted by <u>Davies</u>. For this additional reason, therefore, the combination suggested by the Examiner is not supported by the cited prior art.

With respect to the Examiner's confusion about Appellants' arguments at page 17 of the Appeal Brief, Appellants will clarify the argument made on that page. Appellants mistakenly used the name <u>Davies</u> five lines from the bottom of the page instead of <u>Griffith</u>. The intent was to assert that the secret key cryptosystem of <u>Griffith</u> would not have been used in combination with the public key cryptosystem of <u>Davies</u>. To further clarify, there are two well known encryption systems, public key/private key cryptography systems and secret key cryptography systems. In public key/private key systems, the use of one of the pair of keys to encrypt a message is only decipherable using the other of the pair. Further, one of the pair of keys cannot be determined from knowledge of the other. In such systems, therefore, one key can be used by a first person to encrypt a message which is decipherable to a second person possessing the paired key without the second person having knowledge of the value of the key used for encryption. On the other hand, in secret key systems the same key is used both to encrypt and decrypt a message. In such a system the same key must be known to both the sender and receiver of a message. The Examiner's confusion seems to center around equating a secret key with a private key. <u>See</u> page 12 of the Examiner's

4

Answer. The terms are not correctly interchangeable. Appellants clarify and assert that the combination of the secret key system of <u>Griffith</u> with the public key system of <u>Davies</u> is not supported by the references.

## 2. Group II: Claims 2 and 4

As discussed above with respect to claim 1, <u>Davies</u> fails to teach or suggest a unique human identifier. <u>Davies,</u> therefore, also fails to teach or suggest formatting a unique code, transaction data, and the unique human identifier together to produce a single whole representation of a secure endorsed transaction.

As discussed in the previous responses, the unique code as defined by claim 1 is generated using the transaction data and the unique human identifier. Claim 2, therefore, requires that the unique code created from the transaction data and the unique human identifier are formatted together with the very information used to create the unique code. Neither <u>Griffith</u> nor <u>Davies</u> teaches a step of formatting together a unique code generated using a unique human identifier with the information used to generate the unique code. The Examiner cites <u>Griffith</u> as teaching a unique human identifier, however, <u>Griffith</u> fails to teach or suggest that the disclosed identifier should be used in combination with transaction data to create a unique code and then formatted together with the unique code and the transaction data to create a single whole representation of the transaction.

The Examiner asserts that the "biometric" could be used as an "augmentation to securely identify the presence of an individual at the time the document was created." This argument, however, fails to address why the "biometric" would be used to generate

a unique code and then also formatted together with that unique code to create a single whole representation of the transaction. Specifically, the Examiner fails to address why the value would be used two times in generating a single whole representation. Appellants assert that the prior art cited by the Examiner fails to teach or suggest the claimed combination, and therefore, the rejection of claims 2 and 4 should be withdrawn.

     **B.**     **Claims 5-23 and 29-31 have been improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over <u>Davies</u> in view of <u>Griffith</u> and further in view of <u>Spies</u>.**

### 1. Group III: Claims 5-10 and 20-23

Regarding claims 5-10 and 20-23, as with claim 2 discussed above, a unique code is generated using a unique human identifier and transaction data. As recited in claim 5, the unique code is then transmitted along with the unique human identifier and transaction data used to generate the unique code. As discussed above with respect to claim 2, neither <u>Davies</u> nor <u>Griffith</u> teaches combining together a unique code generated from a unique human identifier and transaction data with the information used to generate the unique code. <u>Spies</u> also fails to teach or suggest such a step. The Examiner's assertion of the obviousness of this step in claim 2 was to suggest that the added security of a biometric would lead a person having ordinary skill in the art to add the biometric of <u>Griffith</u> to the system of <u>Davies</u>. Again, Appellants reiterate that even if the use of the biometric of <u>Griffith</u> in the system of <u>Davies</u> was properly suggested by those references, there is simply no teaching or suggestion of combining

6

the biometric back together with a code generated from that biometric. The Examiner has simply used hindsight in view of Appellants claimed invention in order to meet the claim limitation.

### 3. Group V: Claims 11-14 and 29-31

Regarding these claims, the Examiner deals with these claims using a level of abstraction far to general with respect to the actual limitations of the claims. The question of patentability does not rest upon the general knowledge of elements of the claims in the art, but rather must be reviewed based on the combination of those teachings.

Claim 11 specifically recites "generating a unique code from [ ] transaction data, [a] unique human identifier, and [a] public key, wherein the unique code constitutes a secure endorsement of the transaction by [a] first party; and generating, using a private key correspond to the received public key, a digital signature of the unique code, wherein the digital signature constitutes a secure endorsement of the transaction by [a] second party."

Claim 11, therefore, requires two separate endorsements of the transaction by two separate parties. The Examiner asserts at page 15 of the Examiner's Answer:

> [t]he use of a public key to send data to one individual only is one of the basic teachings of public key cryptography. To make an analogy, if Appellant had applied for a method for providing a stock price over a telephone, and claimed in addition that the phone number of the providing party was first dialed by the quote receiving party, the additional dialing limitation would not make the claim more patentable . . . . So if the first party wants to send the transaction data and a unique human identifier to a second party, such that only the second party may read the transaction

7

data and the unique human identifier, the first party may use the public key of the second party.

Appellants fail to understand the relevance of either the Examiner's analogy or argument regarding the use by the first party of the public key of the second party. Claim 11 does not recite simply sending transaction data and a unique human identifier to a second party, but rather requires the generation of a unique code as a secure endorsement of the transaction by the first party and the generation of a digital signal as a secure endorsement of the transaction by the second party.

None of the references cited by the Examiner remotely teaches or suggests a method involving two separate endorsements of a transaction by two separate parties. The references also fail to teach or suggest that the first endorsement involves the use of a public key and the second endorsement involves the use of a private key corresponding to the public key.

The Examiner seems to suggest that the claim is directed to decryption of a message from a first party using a private key of a second party. The claim does not remotely relate to or recite such elements. The action by the second party in the claimed invention is not a decryption of a message sent by a first party, but rather is the generation of a digital signature as an endorsement to a transaction. Because the Examiner has failed to provide any evidence in the prior art that it was known in the art to provide two endorsements of a transaction in the manner expressly recited in claim 11, that claim is patentable over the cited references.

8

Regarding claims 12-14 and 29-31, these claims are patentable over the cited references, at least, in view of their dependence from claim 11.

### 4. Group VI: Claims 15-18

Regarding claim 15, the Examiner asserts at page 16 of the Office Action that "[t]he verification [of the cited prior art] is basic to public key cryptography, and is taught in both Spies and Schneier . . . In fact, claim 15 is a semantic variation on claim 11. If the transaction data is endorsed using a public key as recited in claim 11, then the decryption process using the secret key corresponding to the public key is the verification process that will allow verification and comparison."

Nowhere in claim 15 does Appellant recite the use of either a public key or a private key. The secure endorsed transaction is comprised of transaction data, a unique human identifier, and a unique code generated from the transaction data and the unique human identifier. The verification process involved regenerating the unique code from the received transaction data and unique human identifier and comparing the regenerated unique code against the received unique code to determine if tampering had occurred.

The claim, therefore, requires a comparison of a received unique code against a generated unique code, *wherein the generated unique code is generated using information received with the received unique code.* As is well known in the art, when private key cryptography is used, the private key is not a received element, but rather must be a stored element, such that the private key remains "private." When a verification is performed using a private key, that verification cannot be performed using

received information as is recited in claim 15, but rather must involve the use of a private key that is known only to the party decrypting the message. Claim 15, therefore, is patentable over the cited references.

Regarding claims 16-18, these claims are patentable over the cited references for at least essentially the same reasons expressed above with respect to claim 15.

### 5. Group VII:  Claim 19

Regarding claim 19, as with claim 11 discussed above, the claimed transaction involves the endorsement by two separate parties, a first party endorses the transaction using a unique human identifier and the second party endorses the transaction using a private key. None of the prior art references cited by the Examiner remotely teaches a process wherein a transaction is endorsed by two parties in the specific manner recited in claims 11 or 19. In claim 19 a verification process is performed, wherein the public key of the second party is used to verify that the private key of the second party was used in generating the digital signature received by the verifying party. Further, the endorsement by the first party is performed by comparing a unique code generated from transaction data and a unique human identifier against a unique code received as part of the digital signature. As with claim 15 discussed above, the verification process performed on the unique code involves the comparison of received information (the unique code) against other information received with the unique code (transaction data and unique human identifier). The prior art references cited by the Examiner alone or in any reasonable combination fail to teach or suggest such a combination of elements.

10

## Conclusion

For the reasons expressed above and for the reasons expressed in the Appeal Brief filed July 21, 2000, Appellants assert that the combination of references cited by the Examiner fail to teach or suggest Appellants invention as expressly recited in the claims. The embodiments of the claimed invention simply are neither taught or suggested in the prior art. The basis for the rejections is impermissible hindsight, wherein the Examiner determines the obviousness of a claimed invention simply to meet the limitations of the pending claims.

In view of the above, Appellants respectfully request a positive determination as to the patentability of Appellants' invention as recited in claims 1-23, 25-27, and 29-31.

If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Reg. No. 24,914

By:     Jeffrey A. Berkowitz
        Reg. No. 36,743

Dated: Sept. 21, 2000

Finnegan, Henderson, Farabow,
    Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, D.C. 20005
(202) 408-4000

11